カメラ、レコーダーなどへの不正アクセスにご注意ください

日頃は、弊社製品をご愛用いただきまして、誠にありがとうございます。

ネットワークカメラ、ネットワークディスクレコーダー等はWebサーバーを内蔵した製品です。インターネット経由で機器にアクセスできるようにすることができますが、使い方によっては第三者が不正にアクセスし、プライバシーや肖像権の侵害、情報漏えいなどが起こるおそれがございます。

インターネット経由で接続できるようにしてお使いの場合、機器の設定やご利用手順を点検されますよう、お勧めします。設定項目や手順などは製品により異なります。

製品ごとの機能や設定手順は、お使いの製品の取扱説明書をご覧ください

[次のような危険な状態で使用されていないか、ご確認ください]

●設定画面で「ユーザー認証」=「off」(機種により「未登録ユーザーを許可」)の設定でご使用の場合、IPアドレスやドメイン名 (例 http://〇〇〇〇.miemasu.net:△△△△) だけで、誰でもアクセスできますので非常に危険です。
ユーザー認証の設定を「On」(機種により「未登録ユーザーを禁止」) にし、容易に推測されない文字と数字を組み合わせてユーザー名・パスワードを設定するとともに、ユーザー名・パスワードは定期的に変更してください。

● 工場出荷時のユーザー名、パスワードを削除せずに使用している場合は、工場出荷時のユーザー名、パスワードは広く公開されていますので大変危険です。容易に推測されない文字と数字を組み合わせてユーザー名・パスワードを設定後、工場出荷時のユーザー名、パスワードを削除してください。また、ユーザー名・パスワードは定期的に変更してください。

● 「11111」などの連続する数字や文字、関係者の生年月日や電話番号などは、容易に知られるおそれがあり危険です。容易に推測されない文字と数字を組み合わせてユーザー名・パスワードを設定するとともに、ユーザー名・パスワードは定期的に変更してください。

● 長期間ユーザー名、パスワードを変更せずに使用するのは危険です。ユーザー名・パスワードは定期的に変更してください。

● 管理者が不明のユーザー名、パスワードが設定されている場合は危険です。不明なユーザー名、パスワードは設定画面で削除してください。

● 管理者のユーザー名、パスワードで機器にアクセスしたあと、ブラウザーのウインドウを一部でも開いたまま放置すると危険です。管理者のユーザー名でログインした場合は、機器のそばを離れないようにし、必要な作業のあとはすぐにログアウトするとともに、すべてのブラウザーのウインドウを閉じてください。やむをえず作業中に機器のそばを離れる場合は、関係者以外が入室できないように対策を講じることをお勧めします。

その他、カメラ、レコーダーあるいはネットワーク機器などの各種のセキュリティ機能を活用し、不正アクセスなどが生じないよう、ご注意ください。

セキュリティのトップページへ